UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: JOSE SOTO, individually and on behalf of all others similarly situated, Plaintiff, v. MILLIMAN SOLUTIONS, LLC, MILLIMAN, INC. (d/b/a MILLIMAN INTELLISCRIPT, INC.), PENSION BENEFIT INFORMATION LLC, MEMBERS LIFE INSURANCE COMPANY, and PROGRESS SOFTWARE CORPORATION, Defendants.	MDL No. 1:23-md-03083-ADB **AMENDED CLASS ACTION COMPLAINT** CIVIL ACTION NO. 1:23-cv-12490

Plaintiff Jose Soto ("Plaintiff") individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to himself and on information and belief as to all other matters, brings this Class Action Complaint against Defendants Milliman, Inc. (d/b/a Milliman Intelliscript, Inc.), Milliman Solutions, LLC ("Milliman Solutions") (collectively with Milliman, Inc., "Milliman"), Pension Benefit Information, LLC ("PBI"), MEMBERS Life Insurance Company ("MLIC"), and Progress Software Corporation ("PSC") (collectively, "Defendants") and in support thereof alleges as follows:

NATURE OF THE ACTION

1. Plaintiff incorporates the allegations contained in Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908) in its entirety.

2. Plaintiff brings this class action on behalf of himself and all other individuals ("class members"), who had their sensitive personal identifiable information ("PII") accessed and hacked by malicious, unauthorized third parties that accessed Defendants' MOVEit Transfer servers and accessed and removed PII from the server as early as May 27, 2023 (the "Data Breach").[1]

3. Milliman describe its business as "provid[ing] risk assessment services to clients including life insurance companies."[2] Its business includes consulting and analyzing cyber security issues, including the threats posed by cyber criminals.[3]

4. Defendant MLIC is a mutual insurance company that offers financial services worldwide.

5. Defendant PBI provides audit and address research services for insurance companies, pension funds, and other organizations, including Milliman.

6. PBI is a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations" and pension plans, and one of the many companies that uses Defendant PSC's MOVEit service to transfer large amounts of data in the ordinary course of its business and the service it provides to pension plans and other organizations.[4]

7. Defendants tout the safety and security of their services on their websites. For instance, Milliman's website states: "We are working with some of the industry's best minds to deploy sophisticated technology such as machine learning, building rapid response solutions that

[1] https://www.reuters.com/technology/hackers-use-flaw-popular-file-transfer-tool-steal-data-researchers-say-2023-06-02/ (last visited August 8, 2023); https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html (last visited August 8, 2023).
[2] MILLIMAN SOLUTIONS, LLC, Data Breach Notification to Maine Attorney General (June 16, 2023).
[3] https://www.milliman.com/en/insurance/cyber (last accessed Aug. 9, 2023).
[4] https://www.pbinfo.com/ (last visited August 1, 2023).

help identify tomorrow's threats, and implementing new approaches to managing risk that actually help people work more efficiently."[5] These comments assuring consumers that their services are safe apply to third-party services that Defendants use in the ordinary course of its business, such as MOVEit.

8. Contrary to their assurances to consumers, however, Defendants lacked adequate systems and procedures for maintaining, safeguarding, and protecting highly sensitive PII entrusted to them. Specifically, on or about July 17, 2023, PBI sent letters to class members, including Plaintiff, informing them that their highly sensitive PII was compromised in the Data Breach that impacted the MOVEit software.[6]

9. Based on their notice of the Maine Attorney General's website, Milliman learned of the Data Breach on June 16, 2023, but inexplicably waited over a month before notifying class members that their highly sensitive PII was compromised thereby.[7]

10. It has been reported that the Data Breach was a ransomware attack conducted by a notorious ransomware group, C10p, which claims to have committed the Data Breach.[8]

11. Defendants owed a non-delegable duty to Plaintiff and class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure.

12. Defendants could have prevented the Data Breach by properly vetting and monitoring their systems, including MOVEit.

---

[5] https://us.milliman.com/en/risk/cyber (last accessed Aug. 9, 2023).
[6] MILLIMAN SOLUTIONS, LLC, Data Breach Notification to Maine Attorney General, *supra*.
[7] https://apps.web.maine.gov/online/aeviewer/ME/40/a98d9ae9-b898-4aaa-8dde-de04551aaedb.shtml
[8] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html

13. By way of example, had Milliman limited the customer information they shared with their vendors and business associates and had Defendants employed reasonable measures to implement and maintain adequate data security measures and protocols to secure and protect Plaintiff's and class members' data, the Breach could have been prevented.

14. Plaintiff and class members entrusted Defendants with, and allowed Defendants to gather, their highly sensitive PII. They did so in confidence, and they had the legitimate expectation that Defendants would respect their privacy and act appropriately, including only sharing their information with those who legitimately needed the information and were equipped to protect it through having adequate processes in place to safeguard it.

15. Trust and confidence are key components of Plaintiff's and class members' relationship with Defendants. Without it, Plaintiff and class members would not have provided Defendants with, or allowed Defendants to collect, their most sensitive information in the first place. To be sure, Plaintiffs and class members relied upon Defendants to keep their information secure, as they are required by law to do.

16. Defendants breached their non-delegable duties to class members by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII entrusted to them from unauthorized access and disclosure, including by ensuring secure services, processes and procedures were in place to safeguard PII that Defendants shared with those third-parties.

17. As a result of Defendants' breaches of their non-delegable duties and obligations, the Data Breach occurred and Plaintiff's and class members' PII was accessed by, and disclosed to, an unauthorized third-party actor. This instant action seeks to remedy these failings and their

consequences. Plaintiff thus brings this complaint on behalf of himself and all similarly situated individuals whose PII was exposed as a result of the Data Breach.

18. Plaintiff, on behalf of himself and all other class members, asserts claims for negligence, negligence per se, invasion of privacy, unjust enrichment, and seeks declaratory and injunctive relief, monetary damages including punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

A. Plaintiff

19. Plaintiff is a resident and citizen of the state of Florida and resides in Saint Cloud, Florida.

20. Plaintiff received a letter from PBI dated July 21, 2023, stating that Plaintiff's PII including his name, address, date of birth, and Social Security number were compromised in the Data Breach.

21. The letter states that PBI provides audit and address research services for insurance companies, including MLIC, and determined that MLIC's customers—including Plaintiff—were among those whose PII was compromised in the Data Breach. Milliman's notice on the Maine Attorney General website explains as follows:

> [Milliman] provide[] risk assessment services to clients including life insurance companies. As part of those services, Milliman Solutions utilizes a third-party vendor, [PBI] …. [Milliman] transferred data regarding its clients' consumers to PBI …. PBI recently notified [Milliman] that PBI experienced a data security incident affecting the data of [Milliman's] clients …. [PBI] confirmed to [Milliman] that the personal information of certain consumers of [Milliman's] clients were affected …. [Milliman's] clients whose consumer data was affected by the incident include MEMBERS Life Insurance Company (MLIC) ….[9]

[9] https://apps.web.maine.gov/online/aeviewer/ME/40/a98d9ae9-b898-4aaa-8dde-de04551aaedb.shtml

Thus, Plaintiff provided his PII to MLIC which, in turn, provided it to Milliman and PBI, where it was subsequently compromised by the Data Breach due to all Defendants' failure to implement and maintain reasonable security procedures and practices to protect the PII entrusted to them from unauthorized access and disclosure, including by ensuring they all had secure services, processes and procedures in place to safeguard PII that Defendants shared amongst themselves.

22. Prior to retaining counsel for claims related to the Data Breach, Plaintiff spent at time monitoring his accounts for fraudulent activity and identity theft. He also spent time contacting the major credit bureaus to freeze his credit. In total, Plaintiff has spent around 10 hours responding to the Breach. He will continue to expend further time doing so in the days, weeks, and months following the filing of this complaint**.**

B. Defendants

23. Defendant Milliman, Inc. is a Washington corporation, with its principal place of business in Seattle, Washington.

24. Defendant Milliman Solutions, LLC is a Delaware corporation, with its principal place of business in Seattle Washington. Milliman Solutions, LLC is a subsidiary of defendant Milliman, Inc.

25. The Milliman is a Vendor Contracting Entity of PBI. (*See* Plfs.' Omnibus Set of Addtl. Pleading Facts, App. A.)

26. Defendant MEMBERS Life Insurance Company is an Iowa corporation with its principal place of business located in Madison, Wisconsin, and is a Vendor Contracting Entity Customer of Milliman. (*Id.*)

27. Defendant PBI is a for-profit Delaware corporation with its principal place of business at 333 S 7th Street, Suite 2400, Minneapolis, MN 55402. PBI uses PSC's MOVEit service

in the regular course of its business acting as a life insurance "sponsor, administrator, or record keeper" "for thousands of organizations."[10]

28. PBI is a PSC Vendor. (*See* Plfs.' Omnibus Set of Addtl. Pleading Facts, App. A.)

29. Defendant PSC is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803. PSC offers the service MOVEit, which experienced the Data Breach underlying Plaintiff's claims.

JURISDICTION AND VENUE

30. This case was originally filed in the United States District Court for the Western District of Washington. This action was transferred to this Court for coordinated or consolidated pretrial proceedings pursuant to 28 U.S.C. § 1407 and Rule 7.1 of the Rules of Procedure of the United States Judicial Panel on Multidistrict Litigation.

31. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000) and is a class action in which one or more class members are citizens of states different from Defendants.

32. The United States District Court for the Western District of Washington has general personal jurisdiction over Defendants because Milliman maintain their headquarters and principal places of business in that judicial District (i.e., in Seattle, Washington), and Defendants have minimum contacts with the State of Washington and conduct substantial business in the State of Washington.

33. The Western District of Washington is the proper venue for this case pursuant to

[10] www.pbinfo.com (last visited Aug. 1, 2023).

28 U.S.C. § 1391 because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in the State of Washington and because Defendants conduct a substantial part of their business within that District. Moreover, Milliman maintain physical offices and principal places of business in that District.

FACTUAL ALLEGATIONS

A. Overview of Defendants

34. Milliman state that "cyber risk is an ever shifting landscape. New vectors and new attacks pose major challenges to businesses trying to keep data systems and people safe."[11]

35. Milliman market themselves as "experts" in cybersecurity, assuring consumers—such as Plaintiff and class members—that they can "quantify the potential financial impacts of cyber risk and can produce cost-benefit analyses and model a variety of possible risk scenarios to find gaps."[12]

36. Milliman claim that they offer "a next-generation cyber risk solution that incorporates a forward-looking approach to modeling how cyber risks occur and propagate[,] provides organizational decision makers and risk managers with a more accurate understanding of current vulnerabilities[, and] helps identify emerging threat vectors before they cause damage[.]"[13]

37. MLIC is a customer of Milliman.

38. Their website repeatedly states that they are keenly cognizant of data privacy risks and have adequate procedures and process in place to prevent them, including their statements that:

[11] MILLIMAN, INC., "CRisALIS for cyber" (video), https://www.milliman.com/en/products/complexriskanalysis (last accessed Aug. 9, 2023).
[12] https://www.milliman.com/en/risk/cyber-risk (last accessed Aug. 9, 2023).
[13] https://www.milliman.com/en/products/complexriskanalysis (last accessed Aug. 9, 2023).

- "We are working with some of the industry's best minds to deploy sophisticated technology such as machine learning, building rapid response solutions that help identify tomorrow's threats, and implementing new approaches to managing risk that actually help people work more efficiently."[14]

- "Any organization that deals with sensitive data faces increasing challenges in keeping that data safe. From guarding against sophisticated cyber criminals to preventing accidental data loss, staying safe means keeping one step ahead."[15]

- "It is essential for any business to rethink how to best model its cyber risk, with the goal of illuminating blind spots instead of missing them."[16]

- "[Cyber risk needs to be analyzed in a way that allows companies to examine the appropriate controls and mitigation techniques, and how causal-based models are a proven way to account for the decisions of both the company and the attacker."[17]

- "From guarding against sophisticated cyber criminals to preventing accidental data loss, staying safe means keeping one step ahead."[18]

- "Cyber risk is evolving fast. You've got to evolve faster."[19]

39. PBI provides audit and address research services for insurance companies, pension funds, and other organizations, including Milliman.

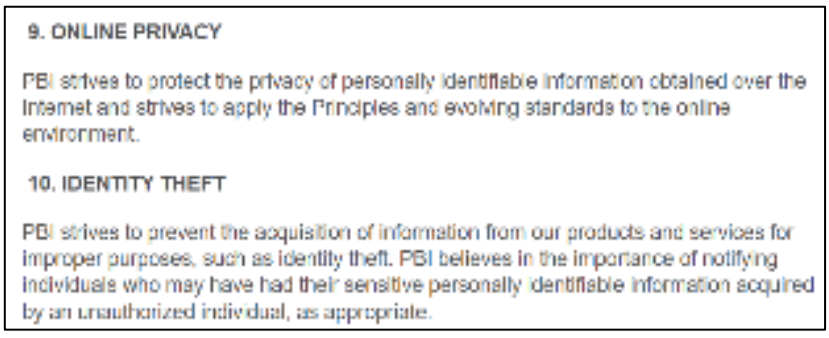
40. PBI is a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations", and one of the many companies that uses PSC's MOVEit service to transfer large amounts of data in the ordinary course of its business and the service it provides to pension plans and other organizations.[20]

[14] https://www.milliman.com/en/insurance/cyber (last accessed Aug. 9, 2023).
[15] https://us.milliman.com/en/risk/cyber (last accessed Aug. 9, 2023).
[16] https://www.milliman.com/en/insight/Know-your-cyber-blind-spots (last accessed Aug. 9, 2023).
[17] https://www.milliman.com/en/insight/does-it-ever-make-sense-for-firms-to-pay-ransomware-criminals (last accessed Aug. 9, 2023).
[18] https://us.milliman.com/en/risk/cyber (last accessed Aug. 9, 2023).
[19] https://www.milliman.com/en/insurance/cyber (last accessed Aug. 9, 2023).
[20] https://www.pbinfo.com/ (last visited August 1, 2023).

41. According to the Notice Letter received by Plaintiff, PBI provides audit and address research services for MLIC.

42. PBI's website also promises consumers that it has robust systems and processes in place to protect and secure their sensitive information:

43. PBI's website also tells consumers that it has systems and process in place to ensure the privacy of their sensitive information obtained over the internet and to prevent identity theft:



44. Furthermore, PBI acknowledges that it has a duty to safeguard Plaintiff's and class members' sensitive PII because, inter alia, PBI's website tells consumers that it has systems

in place to protect consumers' sensitive information, and routinely audits those systems to ensure they are compliant with federal regulations and other legislation—as well as industry standards and practices— governing data privacy:

> **8. ACCOUNTABILITY**
>
> PBI supports accountability of information industry standards and practices, responsible and effective federal regulation of the data industry, and legislation governing the practices of all data providers. PBI also supports industry oversight and active engagement with the privacy community. PBI believes that strong privacy and information security protections are vital for an effective and trusted data industry.
>
> **11. COMPLIANCE**
>
> PBI will obtain assessments from an independent auditor, who uses procedures and standards generally accepted in the profession to assess PBI's controls relevant to security, availability, and confidentiality, as appropriate.

45. Discovery will show that through their provision of the foregoing services, PBI obtains possession of customers'—including Plaintiff's and class members'—highly sensitive PII. Thus, in the regular course of their businesses, PBI collects and/or maintains the PII of consumers such as Plaintiff and class members. PBI stores this information digitally in the regular course of business.

46. As evidenced by, inter alia, their receipt of the notice informing them that their PII were compromised in the Data Breach, Plaintiff's and class members' PII was transferred using PSC's MOVEit service and/or they otherwise entrusted to Defendants their PII, from which Defendants profited.

47. Yet, contrary to PBI's website representations—by virtue of Defendants'

admissions that they experienced the Data Breach—Defendants did not have adequate measures in place to protect and maintain sensitive PII entrusted to it. Instead, Defendants' websites wholly fail to disclose the truth: that Defendants lack sufficient processes to protect the PII that is entrusted to them.

48. In the course of their relationship, clients, including Plaintiff and class members, provided Defendants, directly or indirectly, with at least the following PII:

a. names;
b. dates of birth;
c. Social Security numbers; and
d. addresses.

49. In the course of its ordinary business operations, Defendants are entrusted with safeguarding the sensitive PII of customers.

50. Plaintiff and class members are current or former MLIC customer who provided their PII to Defendants.

51. Based on the foregoing, Defendants were aware that they owed non-delegable duties to Plaintiff and class members to keep their PII safe and secure, which includes duties to ensure that all information Defendants collect, store and/or transfer is secure, and that any associated entities with whom Defendants shared information maintained adequate and commercially reasonable data security practices to ensure the protection of PII within Defendants' possession.

52. Discovery will show that through Defendants' provision of their services, they obtain possession of customers'—including Plaintiff's and class members'—highly sensitive PII. Thus, in the regular course of their businesses, all Defendants collect and/or maintain the PII of consumers such as Plaintiff and class members, and store that information digitally in the regular course of business.

B. The Data Breach

53. Defendants Milliman posted an explanation of the Data Breach on the Maine Attorney General's website that states as follows[21]:

> Milliman Solutions provides risk assessment services to clients including life insurance companies. As part of those services, Milliman Solutions utilizes a third-party vendor, Pension Benefit Information, LLC ("PBI"), to conduct research on whether consumers have passed away. For that purpose, Milliman Solutions transferred data regarding its clients' consumers to PBI utilizing a secure and encrypted file transfer protocol. PBI recently notified Milliman Solutions that PBI experienced a data security incident affecting the data of Milliman Solutions' clients. Specifically, PBI disclosed that it utilized the "MOVEit Transfer" software provided by Progress Software Corporation ("Progress Software") for PBI's secure file transfer protocol ("SFTP") servers. PBI also indicated that it stored Milliman Solutions' clients' data on PBI's SFTP servers utilizing the MOVEit Transfer software. According to information provided to Milliman Solutions by PBI, on or around May 31, 2023, Progress Software disclosed for the first time that its MOVEit Transfer software contained a previously unknown, "zero-day" vulnerability that could be exploited by an unauthorized actor (CVE-2023-34362). PBI also disclosed that it launched an investigation into the nature and scope of the MOVEit vulnerability's impact to PBI's systems. According to PBI, its investigation determined that an unauthorized third party accessed one of PBI's MOVEit Transfer servers on May 29, 2023, and May 30, 2023, and downloaded data. PBI explained it then conducted a manual review of its data to confirm the identities of individuals potentially affected by this event. PBI completed that review on June 16, 2023, and confirmed to Milliman Solutions at that time that the personal information of certain consumers of Milliman Solutions' clients were affected and Milliman Solutions, following reconciliation of the data, was able to recently inform its clients of the scope of individuals whose information may have been affected. The Milliman Solutions clients whose consumer data was affected by the incident include MEMBERS Life Insurance Company (MLIC), CMFG Life Insurance Company ("CMFG"), and The Independent Order of Foresters ("Foresters").

54. Based on the statement on the Maine Attorney General's website, Milliman learned of the Data Breach on June 16, 2023, but inexplicably waited over a month before notifying class members that their highly sensitive PII were compromised thereby.

[21] https://apps.web.maine.gov/online/aeviewer/ME/40/a98d9ae9-b898-4aaa-8dde-de04551aaedb.shtml

55. PBI's letter to Plaintiff states that the Breach originated through a compromise of the MOVEit service. MOVEit is a "managed file transfer software" that companies—such as Defendants—use to transfer files.[22] Defendants use MOVEit in the regular course of their business as described above.

56. Thus, the Data Breach resulted from Defendants' failure to adequately protect and safeguard the highly sensitive PII entrusted to them, including by ensuring secure services, processes and procedures were in place to safeguard PII that Defendants shared with those third-parties.

57. As noted above, it is believed that the Data Breach was a ransomware attack conducted by C10p, which itself claims to have committed the Data Breach.[23]

58. Through its hack of MOVEit, C10p claims to have stolen PII and protected health information ("PHI") from over 550 organizations and 37 million individuals, including U.S. schools, the U.S. public sector, and the U.S. private sector.[24]

59. C10p is a well-known ransomware group, which "[has] been linked to FIN11, a financially-motivated cybercrime operation" and is "connected to both Russia and Ukraine and which is believed to be part of a larger umbrella operation known as TA505."[25]

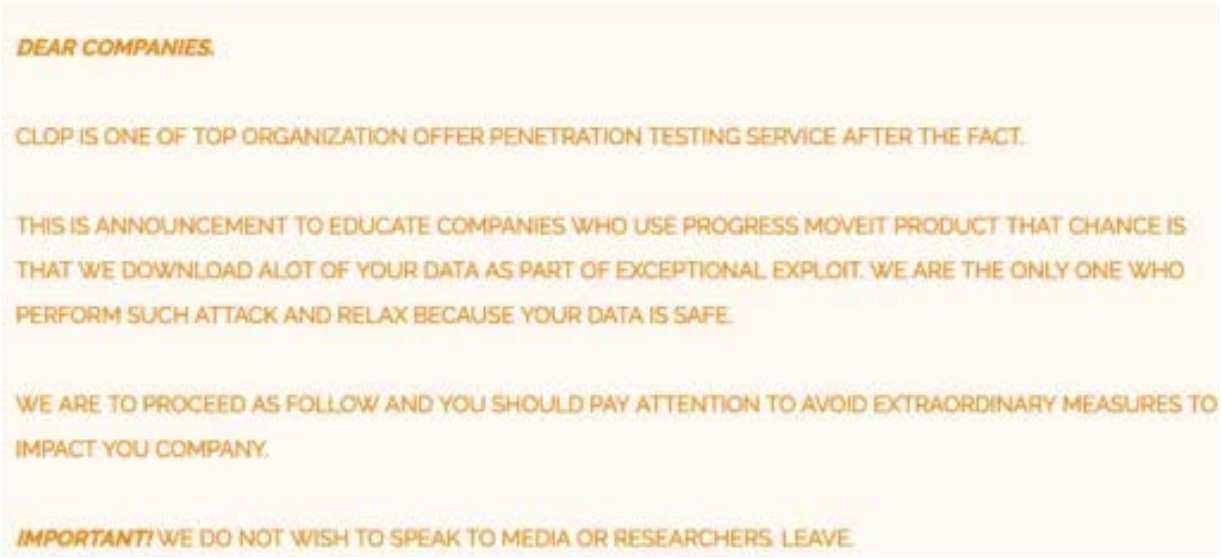
60. It has been reported that C10p has requested unspecified ransom from organizations impacted by MOVEit breaches in exchange for C10p to abstain from releasing consumers' highly sensitive PII and PHI.

---

[22] https://www.ipswitch.com/moveit?_ga=2.178322852.1251772019.1689781398-357640369.1688748444 (last visited August 1, 2023).
[23] https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/ (last visited June 12, 2024).
[24] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html
[25] *Id*.

61. As of July 19, 2023, C10p and its hacking of MOVEit has resulted in the theft of more than 37 million individuals' sensitive information.[26]

62. C10p posted a statement on its website demanding ransom from all companies impacted by the MOVEit breach, which includes the present Data Breach, stating that if they refused to pay the ransom, C10p would post the sensitive PII and PHI stolen from Defendants' systems on the dark web[27]:



DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

[26] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html
[27] *See supra* n.46.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

63. Because the Data Breach was conducted by known, self-proclaimed ransomware cybercriminals, Plaintiff's and class members' sensitive PII is irrefutably in the possession of known bad actors. Furthermore, based on C10p's statement above, Plaintiff's and class members' PII may have already been published, which places them at imminent risk that their data will be misused.

64. As explicitly acknowledged and stated on their own websites, Defendants owed non-delegable duties to Plaintiff and class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access

and disclosure, and to promptly notify individuals of any breach involving their information. Defendants breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect PII from unauthorized access and disclosure, including by ensuring they all had secure services, processes and procedures in place to safeguard PII.

65. There were multiple things Defendants could have done—and were obligated to do—to ensure all had secure services, processes, and procedures in place to safeguard PII that was provided to them, which would have prevented the Data Breach, but Defendants simply opted not to do them. For instance, as one leading cybersecurity expert explained, Defendants should have done the following when utilizing MOVEit. These steps, alongside others, could have ensured the sensitive PII Defendants transferred through MOVEit remained secure and free from data breach:

- "MOVEit should be behind technologies that provide access to only those who need it via tools such as Zero Trust (e.g. access gateways secured by MFA) or simple allowlists and blocklists."[28]
- "If you run MOVEit within your organization, ensure that the database runs as a specific user that can only interact with MOVEit and not as a superuser with broader access. The exploit utilizes SQL injection to allow attackers to manipulate server databases and execute arbitrary code, resulting in data exfiltration. Because this breach is an SQL injection leading to remote code execution (RCE), the adversary only gains initial access to the database server and user."[29]

[28] https://securityscorecard.com/blog/three-steps-to-avoid-moveit-exploit/
[29] *Id.*

Defendants also could have employed (either internally or through third parties) competent professionals to act as 24/7 "eyes on glass." Providers of managed security services, also referred to as "managed detection and response" ("MDR") employ a sophisticated series of artificial and human intelligence to monitor for signs that a breach is underway.

66. Defendants could and should have been monitoring their own systems and repositories for indications of compromise ("IOCs.") It has been reported, for example, that the MOVEIT vulnerability was exploited by C10p "injecting" SQL computer code in order to execute a series of commands that ultimately resulted in the exfiltration of data. But companies have an obligation to monitor their systems for the execution of unauthorized code. If Defendants had had appropriate monitoring in place, they could have detected, and prevented this attack.

67. Companies who were using appropriate managed security detected the MOVEIT vulnerability as early as May 27, 2023, and were able to take steps to prevent the large scale exfiltration of consumers' sensitive information. For instance, on May 27, 2023, as part of C10P's attack of MOVEit, "Akamai researchers detected exploitation attempts against one of Akamai's financial customers — an attack that was blocked by the Akamai Adaptive Security Engine."[30] Thus, services were available for Defendants to detect the Data Breach and prevent large scale exfiltration of PII entrusted to Defendants, but Defendants simply failed to appropriately implement these services. Furthermore, it does not take cybersecurity expertise to know Defendants should not have maintained—or allowed the maintenance of—millions of consumers' PII on MOVEit software, where it was a sitting duck waiting for a cyberattack such as the Data

[30] https://www.akamai.com/blog/security-research/moveit-sqli-zero-day-exploit-clop-ransomware

Breach. In sum, there were plenty of technologies and processes readily available that Defendants could have utilized to prevent the Data Breach, but Defendants failed to do so.

C. Defendants Knew that Criminals Target PII

68. At all relevant times, Defendants knew, or should have known, customers' clients'—such as Plaintiff's and all other class members'—PII was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and class members' PII from cyber-attacks that Defendants should have anticipated and guarded against.

69. PII is a valuable property right.[31] The value of PII as a commodity is measurable.[32] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[33] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[34] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

70. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII and other sensitive

[31] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data

[32] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[33] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[34] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

71. Consumers place a high value on the privacy of their PII. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[35]

72. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

D. Theft of PII Has Grave and Lasting Consequences for Victims

73. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, start new utility accounts, and incur charges and credit in a person's name.[36]

74. Identity thieves use PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[37] According to Experian, one of the largest credit

[35] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[36] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 15, 2021).

[37] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or

reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[38]

75. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[39]

76. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[40]

77. Theft of SSNs also creates a particularly alarming situation for victims because

---

taxpayer identification number. *Id.*

[38] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[39] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Nov. 15, 2021).

[40] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Nov. 15, 2021).

those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

78. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[41]

79. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[42]

80. It is within this harsh and dangerous reality that Plaintiff and all other Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

E. Damages Sustained by Plaintiff and the Other Class Members

81. As a direct and proximate result of Defendants' failures alleged above, Plaintiff and class members are at substantial risk of suffering identity theft and fraud or misuse of their PII.

82. Plaintiff and the class members suffered actual injury from having PII compromised

[41] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[42] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

as a result of Defendants' negligent security processes and procedures and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PII, a form of property that Defendants obtained from Plaintiff; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

83. For the reasons mentioned above, Defendants' conduct, which directly and proximately caused the Data Breach, caused Plaintiff and class members these significant injuries and harm.

84. Plaintiff brings this class action against Defendants for their failure to: (1) properly secure and safeguard PII; (2) ensure that proper security measures were in place to protect PII; (3) ensure secure services, processes and procedures were in place to safeguard PII; and (4) provide timely, accurate, and adequate notice to Plaintiff and other class members that their PII had been compromised.

CLASS ALLEGATIONS

85. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

86. Specifically, Plaintiff proposes the following classes:

(1) PSC Nationwide Class: All persons whose PII was compromised in the MOVEit data breach.

   (a) PSC Florida Class: All residents of Florida whose PII was compromised in the MOVEit data breach.

(2) PBI Nationwide Class: All persons whose PII was compromised on PBI's platform and/or systems in the MOVEit data breach.

   (a) PBI Florida Class: All residents of Florida whose PII was compromised on PBI's platform and/or systems in the MOVEit data breach.

(3) MLIC Nationwide Class: All persons whose PII was compromised in the MOVEit data breach where such PII was obtained from or hosted by MLIC.

(a) MLIC Florida Class: All residents of Florida whose PII was compromised in the MOVEit data breach where such PII was obtained from or hosted by MLIC.

(4) Milliman Nationwide Class: All persons whose PII was compromised in the MOVEit data breach where such PII was obtained from or hosted by Milliman.

(b) Milliman Florida Class: All residents of Florida whose PII was compromised in the MOVEit data breach where such PII was obtained from or hosted by Milliman.

The foregoing nationwide classes are referred to as the "Nationwide Classes" and the state classes are referred to as the "Florida Classes."

87. The foregoing classes are referred to herein, collectively, as the "Classes." Excluded from the Classes are: (1) the judges presiding over the action, Class Counsel, and members of their families; (2) the Defendants, their subsidiaries, parent companies, successors, predecessors, and any entity in which Defendants or their parents have a controlling interest, and their current or former officers and directors; (3) persons who properly opt out; and (4) the successors or assigns of any such excluded persons.

88. **Numerosity**: Class members are so numerous that their individual joinder is impracticable, as the proposed Classes include millions who are geographically dispersed.

89. **Typicality**: Plaintiff's claims are typical of class members' claims. Plaintiff and all class members were injured through Defendants' uniform misconduct, and Plaintiff's claims are identical to the claims of the class members he seeks to represent.

90. **Adequacy**: Plaintiff's interests are aligned with the Classes he seeks to represent and Plaintiff has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and his

counsel intend to prosecute this action vigorously. The Classes' interests are well-represented by Plaintiff and undersigned counsel.

91. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other class members' claims. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for class members individually to effectively redress Defendants' wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

92. **Commonality and Predominance:** The following questions common to all class members predominate over any potential questions affecting individual class members:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and class members' PII from unauthorized access and disclosure;

b. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and class members' PII;

c. Whether Defendants breached their duties to protect Plaintiff's and class members' PII;

d. Whether Plaintiff and all other class members are entitled to damages and the

measure of such damages and relief.

93. Given that Defendants engaged in a common course of conduct as to Plaintiff and the Classes, similar or identical injuries and common law violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Classes or, Alternatively, the Florida Classes, Against All Defendants)

94. Plaintiff realleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs.

95. Defendants owed duties to Plaintiff and all other class members to exercise reasonable care in safeguarding and protecting their PII in Defendants' possession, custody, or control, including non-delegable duties to safeguard that PII. This duty could not be delegated; rather, Defendants had an independent obligation to control all environments into which they placed consumers' PII, and to ensure that those environments were used, configured and monitored in such a way as to ensure the safety of consumers' data.

96. Defendants owed duties to Plaintiff and class members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and class members' PII within their control from being compromised, lost, stolen, accessed and misused by unauthorized persons.

97. Defendants owed a duty of care to Plaintiff and class members to provide security, consistent with industry standards, to ensure that the systems and networks adequately protected the PII.

98. Defendants knew the risks of collecting and storing Plaintiff's and all other class members' PII and the importance of maintaining secure systems and ensuring all Defendants had secure services, processes and procedures in place to safeguard that PII. Defendants knew of the many data breaches that targeted PII, especially SSNs, in recent years.

99. Given the nature of Defendants' businesses, the sensitivity and value of the PII they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

100. Defendants breached their duties in numerous ways, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and class members' PII;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

c. Failing to comply with regulations protecting the PII at issue during the period of the Data Breach;

d. Failing to adequately monitor and audit the data security systems of its vendors and business associates such as the MOVEit service;

e. Failing to recognize in a timely manner that Plaintiff's and class members' PII had been compromised; and

f. Failing to timely and adequately disclose that Plaintiff's and class members' PII had been improperly acquired or accessed.

101. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PII by failing to control, design,

adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols to ensure that all software and hardware systems into which they placed consumers' data were protected against the unauthorized release, disclosure, and dissemination of Plaintiff's and class members' PII.

102. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and class members, their PII would not have been compromised.

103. As a result of Defendants' above-described wrongful actions, inactions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other class members have suffered, and will continue to suffer, economic damages and other injuries and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—a risk that justifies expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost value of the unauthorized access to their PII permitted by Defendants; (vi) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach; and/or (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Nationwide Classes or, Alternatively, the Florida Classes, Against All Defendants)

104. Plaintiff realleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs.

105. Defendants' duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted

by the FTC, the unfair act or practice by a business, such as Defendants, of failing to employ reasonable measures to protect and secure PII.

106. Defendants violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other class members' PII and not complying with applicable industry standards, including by failing to control all environments into which they placed consumers' PII, and to ensure that those environments were used, configured and monitored in such a way as to ensure the safety of consumers' data. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtain and store, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and the other class members.

107. Defendants' violations of Section 5 of the FTCA constitute negligence per se.

108. Plaintiff and class members are within the class of persons that Section 5 of the FTCA were intended to protect.

109. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA were intended to guard against.

110. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and class members' PII to unauthorized individuals.

111. The injury and harm that Plaintiff and the other class members suffered was the direct and proximate result of Defendants' violations of Section 5 of the FTCA. Plaintiff and class

members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost value of the unauthorized access to their PII permitted by Defendants; (vi) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach; and/or (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT III
INVASION OF PRIVACY
(INTRUSION UPON SECLUSION)
(On Behalf of Plaintiff and the Nationwide Classes or, Alternatively, the Florida Classes, Against All Defendants)

112. Plaintiff realleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs.

113. Plaintiff and class members had a reasonable expectation of privacy in the PII that Defendants failed to safeguard and allowed to be accessed by way of the Data Breach.

114. Defendants' conduct as alleged above intruded upon Plaintiff's and class members' seclusion under common law.

115. By intentionally and/or knowingly failing to keep Plaintiff's and class members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants intentionally invaded Plaintiff's and class members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and class members' private affairs in a manner that identifies Plaintiff and class members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and class members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and class members.

116. Defendants knew that an ordinary person in Plaintiff's and a class member's position would consider Defendants' intentional actions highly offensive and objectionable.

117. Defendants invaded Plaintiff and class members' right to privacy and intruded into Plaintiff's and class members' seclusion by intentionally failing to safeguard, misusing, and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

118. Defendants intentionally concealed from Plaintiff and class members an incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

119. As a proximate result of such intentional misuse and disclosures, Plaintiff's and class members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendants' conduct, amounting to a substantial and serious invasion of Plaintiff's and class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendants' intentional actions or inaction highly offensive and objectionable.

120. In failing to protect Plaintiff's and class members' PII, and in intentionally misusing and/or disclosing their PII, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiff's and class members' rights to have such information kept confidential and private.

121. As a direct and proximate result of the foregoing conduct, Plaintiff seeks an award of damages on behalf of himself and the class members.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Classes or, Alternatively, the Florida Classes, Against All Defendants)

122. Plaintiff realleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs.

123. Plaintiff and class members have both a legal and equitable interest in their PII that was collected by, stored by, and maintained by Defendants—thus conferring a benefit upon Defendants—that was ultimately compromised by the Data Breach.

124. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and class members. Defendants also benefitted from the receipt of Plaintiff's and class members' PII.

125. As a result of Defendants' failure to safeguard and protect PII, Plaintiff and class members suffered actual damages.

126. Defendants should not be permitted to retain the benefit belonging to Plaintiff and class members because Defendants failed to adequately implement the data privacy and security procedures that were mandated by federal, state, and local laws and industry standards.

127. Defendants should be compelled to provide for the benefit of Plaintiff and class members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT V
DECLARATORY RELIEF
(28 U.S.C. § 2201)
(On Behalf of Plaintiff and the Nationwide Classes or, Alternatively, the Florida Classes, Against All Defendants)

128. Plaintiff realleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs.

129. An actual controversy has arisen and exists between Plaintiff and class members, on the one hand, and Defendants on the other hand, concerning the Data Breach and Defendants' failure to protect Plaintiff's and class members' PII, including with respect to the issue of whether Defendants took adequate measures to protect that information. Plaintiff and the class members are entitled to judicial determination as to whether Defendants have performed and are adhering to all data privacy obligations as required by law or otherwise to protect Plaintiff's and class members' PII from unauthorized access, disclosure, and use.

130. A judicial determination of the rights and responsibilities of the parties regarding Defendants' privacy policies and whether they failed to adequately protect PII is necessary and appropriate to determine with certainty the rights of Plaintiff and the class members, and so that there is clarity between the parties as to Defendants' data security obligations with respect to PII going forward, in view of the ongoing relationships between the parties.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Classes, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as Class Representative and undersigned counsel as Class Counsel;

B. Award Plaintiff and the Classes actual and statutory damages, punitive damages, nominal damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that class members have an effective remedy, including enjoining Defendants from continuing the unlawful practices as set forth above;

D. Award Plaintiff and the Classes pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and the Classes reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and the Classes such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: June 12, 2024

Respectfully submitted,

/s/ Kristen A. Johnson

Kristen A. Johnson (BBO# 667261)
HAGENS BERMAN SOBOL SHAPIRO LLP
1 Faneuil Hall Square, 5th Fl.
Boston, MA 02109
Tel: (617) 482-3700
Fax: (617) 482-3003
kristenj@hbsslaw.com

Plaintiffs' Liaison & Coordinating Counsel

Beth E. Terrell, WSBA #26759
Email: bterrell@terrellmarshall.com
936 North 34th Street, Suite 300
Seattle, Washington 98103
Telephone: (206) 816-6603
Facsimile: (206) 319-5450

E. Michelle Drake
BERGER MONTAGUE, PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
Email: emdrake@bm.net

Mark B. DeSanto
BERGER MONTAGUE, PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel: (215) 875-3000
Fax: (215) 875-4604
Email: mdesanto@bm.net

Norman E. Siegel
Barrett J. Vahle
J. Austin Moore
Jillian R. Dent
Brandi S. Spates
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com
dent@stuevesiegel.com
spates@stuevesiegel.com

Attorneys for Plaintiff

E. Michelle Drake
BERGER MONTAGUE, PC
1229 Tyler St., NE, Ste. 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
emdrake@bm.net

Gary F. Lynch
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Fl.
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
Gary@lcllp.com

Douglas J. McNamara
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW, 5th Fl.
Washington, DC 20005
Tel: (202) 408-4600

dmcnamara@cohenmilstein.com

Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Ave. S., Ste. 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 612-339-0981
khriebel@locklaw.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Ste. 500
Philadelphia, PA 19106
Tel: (215) 592-1500
Fax: (215) 592-4663
cshaffer@lfsblaw.com

Plaintiffs' Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that, on this date, the foregoing document was served by filing it on the Court's CM/ECF system, which will automatically send a notification of such filing to all counsel of record via electronic mail.

Dated: June 12, 2024

/s/ Kristen A. Johnson
Kristen A. Johnson